UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/598,509 | 05/16/2007 | Richard Michael Wyn Harran | GB920040005US1 | 6651 |

76046 7590 04/10/2009

KUNZLER & MCKENZIE
8 EAST BROADWAY
SUITE 600
SALT LAKE CITY, UT 84111

| EXAMINER | |
|---|---|
| VAUGHAN, MICHAEL R | |
| ART UNIT | PAPER NUMBER |
| 2431 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 04/10/2009 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/598,509 | HARRAN ET AL. | |
| | Examiner | Art Unit | |
| | MICHAEL R. VAUGHAN | 2431 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *10 February 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1,39-52 and 54* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 39-52, and 54* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

The instant application having Application No. 10/598509 is presented for examination by the examiner. Claims 1, 39-52, and 54 are pending. Claim 53 has been canceled. Claims 1, 39, 42-44, 50, and 54 have been amended.

## *Response to Amendment*

### *Specification*

The amended specification and title are accepted.

### *Claim Objections*

Claims 1 and 39 are objected to because of the following informalities:

Each of these claims defined a processor and a memory twice.

### *Claim Rejections - 35 USC § 101*

The current amendment overcomes the previous 101 rejection.

### *Claim Rejections - 35 USC § 112*

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1, 39-52, and 54 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The relationship between the idleness and heartbeat is still too loosely coupled to definitively point out the claimed invention. Please see remarks in the section "Response to Arguments" below for more explanation.

As per claim 1, the previously idle communications link lack antecedent basis. If no data has flown it appears the communication is still idle. Appropriate correction is required.

As per claims 39, 44, and 50, there is a step of encoding part of the data. The preambles all recite encrypting data. Encoding and encrypting have different meaning in the art. Are the claims describing encoding or encrypting. Also the preamble says a secret key is for encrypting and the new secret key is for encoding. Do the keys have separate functions?

As per claim 50, a predetermined period of time is defined twice.

As per claim 51, these limitations are already in claim 50, so it is unclear why they are being recited again. Are these functions being performed a second time?

## *Response to Arguments*

Applicant's arguments filed 2/10/09 with respect to the prior art of Parisien and Mamros applied to the claims have been fully considered but they are not persuasive.

Applicant has argued the combination of them under 103 fails to teach the claimed inventions. Examiner with respect to Applicant's allegation that the Examiners agreed to certain proposed claim amendments would overcome the prior art is respectfully traversed. In the interview summary filed 2/17/09, Examiner explicitly states no specific agreement was reached. What Applicant may be misunderstanding is that some features in the specification discussed by Applicant were not found in the prior art but those features needed to be clearly inserted into the claims. At this time there no limitations in the claims which are not taught or suggested by the combination of Parisien and Mamros.

The independent claims are still not in a definitive form which distinctly claims the invention. There are too many ways to interpret some of the features because of there loosely claimed relationship. For example the notion of the link being idle by detecting a heartbeat is ambiguous. In the art, links go idle all of the time. It is inherent that links will become idle. Heartbeats can also contain useful data in them. Therefore having a heartbeat containing data seems to be in conflict with the notion of idleness where nothing is happening. The claims are still too broad in the scope to definitively say which party is sending the heartbeat and why it was sent. The claim simply states that a heartbeat flowed across the communications links. Who sent it? So one major problem with understanding the claims is the relationship between the idle link and the heartbeat.

Another problem with the claim is that the whole method or system of what is being performed is not claimed. Examiner is using Figs 1a and 1b to try to understand

what is being claimed. Figure 1a has parts which seem important to the invention that are not claimed in the independent claims. For example the roles of the timer, heartbeat issuer, and byte measurer are critical in facilitating secure data communications using a secret key. From Figure 1b it is unclear where data is being transmitted. Looking to the claims this step is omitted as well.

From the specification, this invention has merit in a network in which data is intermittingly transferred. It seems the features of the invention would not be triggered in a general network where data is sent with regularity before the connection is torn down. The claims are presented in a general network link without bringing this intermittence to the forefront. Claiming these features in the specific context would go along way in making it clear why these limitations are necessary and how they achieve the goal of reducing overhead.

Without these aforementioned distinct features, the claims as examined do not require more than is taught by the combination of Parisien and Mamros. Parisien teaches refreshing key during idle times. Mamros teaches the notion of heartbeats to preserve a communication link. The combination of Parisien and Mamros seems to teach and achieve the same goal of the claims. That goal being the reduction of unnecessary key refreshes by using changing the keys only every so often and not while data is being transmitted but instead in idle times.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 39-52, and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over USP 6,795,555 to Parisien et al., hereinafter Parisien in view of EP 0999673 to Mamros et al., hereinafter Mamros.

As per claim 1, Parisien teaches a method for facilitating secure data communications using a secret key for encrypting data flowing between first and second entities over a communications link (Fig. 1), the method comprising: determining that the communications link is idle (col. 4, lines 37-38);

determining that there is data to flow over the idle communications link (col. 2, lines 5-10); and

responsive to determining that there is data to flow over the previously idle communications link and determining that the communication link is idle, initiating generation of a new secret key, the new secret key for encrypting data sent between the first and the second entities over the communications link (col. 5, lines 30-35). Parisien is silent in explicitly teaching that a heartbeat indicates the communication link is idle. Mamros teaches the use of heartbeat as a means to keep an idle link open. Heartbeats

are then a way to know that a link is idle and should not be closed. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to use the heartbeats of Mamros to signify a link is idle because it would allow the connection to say open without having to reinitialize the link when the client is still actively present.

As per claim 39, Parisien teaches a method performed at a first entity for facilitating secure data communications by using a secret key for encrypting data flowing between said first and a second entity over a communications link, the method comprising the steps of:

determining that the communications link has been idle (col. 4, lines 37-38);

determining whether data is available for flow over the previously idle communications link (col. 2, lines 5-10); and

in response to a determination that data is available, initiating generation of a new secret key for use in encoding at least part of the available data before it flows onto the communications link (col. 5, lines 30-35). Parisien is silent in explicitly teaching that a heartbeat indicates the communication link is idle. Mamros teaches the use of heartbeat as a means to keep an idle link open. Heartbeats are then a way to know that a link is idle and should not be closed. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to use the heartbeats of Mamros to signify a link is idle because it would allow the connection to say open without having to reinitialize the link when the client is still actively present.

As per claim 40, Parisien is silent in disclosing the step of determining that the link has been idle for at least a predetermined period of time and the step of initiating

generation of a new secret key is performed only if the communications link is found to have been idle for at least the predetermined period of time. Mamros teaches changing keys after a predetermined time (0032). Parisien does teach that only when the communication is idle do the keys get updated. Mamros teaches the notion of measuring the amount of time between key updates so avoid unnecessary overhead (0032). Thus is it important not to needlessly generate new keys close too close to one another. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the teachings of Mamros into the teachings of Parisien because it would alleviate too frequent key updates and therefore save processing time and computation overhead.

As per claim 41, Parisien is silent in disclosing determining whether the amount of data sent over the communications link since the last generation of a secret key exceeds a predetermined amount threshold; and if the amount of data sent exceeds the predetermined amount threshold, initiating generation of a new secret key. Mamros teaches determining whether the amount of data sent over the communications link since the last generation of a secret key exceeds a predetermined amount threshold; and if the amount of data sent exceeds the predetermined amount threshold, initiating generation of a new secret key (0032). It is well known in the art that the longer you use a key the more susceptible it becomes to attach. One of ordinary skill knows this and knows that is why you change keys frequently. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Mamros'

teaching into the system of Parisien. Updating the key after a transmission threshold lowers the chance of the key being discovered by an attacker.

As per claim 42, Parisien is silent in disclosing sending a heartbeat message to the second entity only if it is determined that the link has been idle has been idle for at least the predetermined period of time and that there is no data available for flow over the communications link; and monitoring the communications link for receipt of an acknowledgement from the second entity. Mamros teaches sending a heartbeat message to the second entity only if it is determined that the link has been idle has been idle for at least the predetermined period of time and that there is no data available for flow over the communications link; and monitoring the communications link for receipt of an acknowledgement from the second entity (0038). Mamros teaching is simply a means to prevent premature session ending by sending heartbeat [keep-alive] message between sender and receiver. This method is well known in the art. It is obvious to apply known techniques to known methods which yield predictable results. Therefore the claim would have been obvious because heartbeat messages were recognized as parts of the ordinary capabilities of one skill in the art at the time of the invention.

As per claim 43, Parisien is silent in disclosing the additional step terminating the communications link with the second entity if no acknowledgement is received from the second entity within a predetermined period of time. Mamros teaches the additional step terminating the communications link with the second entity if no acknowledgement is received from the second entity within a predetermined period of time (0039). Examiner supplies the same rationale for combining Mamros and Parisien as recited in

the previous rejection. The use of a heartbeat is to know the other party is still available. It would be obvious to terminate the session if the heartbeat is not acknowledged.

As per claim 44, Parisien teaches an apparatus for facilitating secure data communications by using a secret key to encrypt data flowing over a communications link between the apparatus and a remote system, said apparatus comprising:

a data detector for determining whether the communications link has been idle and whether data is now available for flow to the remote system over the communications link (col. 4, lines 37-38);

key generation logic responsive to determinations that the communications link has been idle and there is data now available for flow to the remote system to initiate generation of a new secret key for use in encoding at least part of the available data before it flows onto the communications link (col. 5, lines 30-35). Parisien is silent in explicitly teaching that a heartbeat indicates the communication link is idle. Mamros teaches the use of heartbeat as a means to keep an idle link open. Heartbeats are then a way to know that a link is idle and should not be closed. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to use the heartbeats of Mamros to signify a link is idle because it would allow the connection to say open without having to reinitialize the link when the client is still actively present.

As per claim 45, Parisien is silent in disclosing the step of determining that the link has been idle for at least a predetermined period of time and the step of initiating generation of a new secret key is performed only if the communications link is found to

have been idle for at least the predetermined period of time. Mamros teaches changing keys after a predetermined time (0032). Parisien does teach that only when the communication is idle do the keys get updated. Mamros teaches the notion of measuring the amount of time between key updates so avoid unnecessary overhead (0032). Thus is it important not to needlessly generate new keys close too close to one another. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the teachings of Mamros into the teachings of Parisien because it would alleviate too frequent key updates and therefore save processing time and computation overhead.

As per claim 46, Parisien is silent in disclosing determining whether the amount of data sent over the communications link since the last generation of a secret key exceeds a predetermined amount threshold; and if the amount of data sent exceeds the predetermined amount threshold, initiating generation of a new secret key. Mamros teaches determining whether the amount of data sent over the communications link since the last generation of a secret key exceeds a predetermined amount threshold; and if the amount of data sent exceeds the predetermined amount threshold, initiating generation of a new secret key (0032). It is well known in the art that the longer you use a key the more susceptible it becomes to attach. One of ordinary skill knows this and knows that is why you change keys frequently. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Mamros' teaching into the system of Parisien. Updating the key after a transmission threshold lowers the chance of the key being discovered by an attacker.

As per claims 47 and 48, Parisien is silent in disclosing sending a heartbeat message to the second entity only if it is determined that the link has been idle has been idle for at least the predetermined period of time and that there is no data available for flow over the communications link; and monitoring the communications link for receipt of an acknowledgement from the second entity. Mamros teaches sending a heartbeat message to the second entity only if it is determined that the link has been idle has been idle for at least the predetermined period of time and that there is no data available for flow over the communications link; and monitoring the communications link for receipt of an acknowledgement from the second entity (0038). Mamros teaching is simply a means to prevent premature session ending by sending heartbeat [keep-alive] message between sender and receiver. This method is well known in the art. It is obvious to apply known techniques to known methods which yield predictable results. Therefore the claim would have been obvious because heartbeat messages were recognized as parts of the ordinary capabilities of one skill in the art at the time of the invention.

As per claim 50, Parisien teaches a program product comprising a computer usable media embodying program (col. 7, line 30) instructions which, when executed in a computer, results in the computer facilitating secure data communications with a remote system by using a secret key for encrypting data flowing between the computer and the remote system over a communications link by:

determining that the communications link has been idle (col. 4, lines 37-38);

determining whether data is available for flow over the previously idle communications link (col. 2, lines 5-10); and

only in response to a determination that data is available for flow over the idle communication link, initiating generation of a new secret key for use in encoding at least part of the available data before it flows onto the communications link such that generation of a new secret key exclusively occurs when data is available for flow over the idle communication link (col. 5, lines 30-35).

Parisien is silent in disclosing sending a heartbeat message to the second entity only if it is determined that the link has been idle has been idle for at least the predetermined period of time and that there is no data available for flow over the communications link and monitoring the communications link for receipt of an acknowledgement from the second entity. Mamros teaches sending and detecting a heartbeat message to the second entity only if it is determined that the link has been idle has been idle for at least the predetermined period of time and that there is no data available for flow over the communications link; and monitoring the communications link for receipt of an acknowledgement from the second entity (0038). Mamros teaching is simply a means to prevent premature session ending by sending heartbeat [keep-alive] message between sender and receiver. This method is well known in the art. It is obvious to apply known techniques to known methods which yield predictable results. Therefore the claim would have been obvious because heartbeat messages were recognized as parts of the ordinary capabilities of one skill in the art at the time of the invention. Mamros teaches changing keys after a predetermined time (0032). Parisien does teach that only when the communication is idle do the keys get updated. Mamros teaches the notion of measuring the amount of time between key updates so avoid

unnecessary overhead (0032). Thus is it important not to needlessly generate new keys close too close to one another. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the teachings of Mamros into the teachings of Parisien because it would alleviate too frequent key updates and therefore save processing time and computation overhead.

As per claim 51, Parisien is silent in disclosing the step of determining that the link has been idle for at least a predetermined period of time and the step of initiating generation of a new secret key is performed only if the communications link is found to have been idle for at least the predetermined period of time. Mamros teaches changing keys after a predetermined time (0032). Parisien does teach that only when the communication is idle do the keys get updated. Mamros teaches the notion of measuring the amount of time between key updates so avoid unnecessary overhead (0032). Thus is it important not to needlessly generate new keys close too close to one another. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the teachings of Mamros into the teachings of Parisien because it would alleviate too frequent key updates and therefore save processing time and computation overhead.

As per claim 52, Parisien is silent in disclosing determining whether the amount of data sent over the communications link since the last generation of a secret key exceeds a predetermined amount threshold; and if the amount of data sent exceeds the predetermined amount threshold, initiating generation of a new secret key. Mamros teaches determining whether the amount of data sent over the communications link

since the last generation of a secret key exceeds a predetermined amount threshold; and if the amount of data sent exceeds the predetermined amount threshold, initiating generation of a new secret key (0032). It is well known in the art that the longer you use a key the more susceptible it becomes to attach. One of ordinary skill knows this and knows that is why you change keys frequently. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Mamros' teaching into the system of Parisien. Updating the key after a transmission threshold lowers the chance of the key being discovered by an attacker.

As per claim 54, Parisien is silent in disclosing the additional step terminating the communications link with the second entity if no acknowledgement is received from the second entity within a predetermined period of time. Mamros teaches the additional step terminating the communications link with the second entity if no acknowledgement is received from the second entity within a predetermined period of time (0039). Examiner supplies the same rationale for combining Mamros and Parisien as recited in the previous rejection. The use of a heartbeat is to know the other party is still available. It would be obvious to terminate the session if the heartbeat is not acknowledged.

***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/Ayaz R. Sheikh/

Supervisory Patent Examiner, Art Unit 2431